International Journal of Advancement in Engineering Technology, Management & Applied Science

Volume 1, Issue 5 October 2014 ISSN No: 2349-3224

Intrusion Detection System in Campus Network: SNORT – the most powerful Open Source Network Security Tool

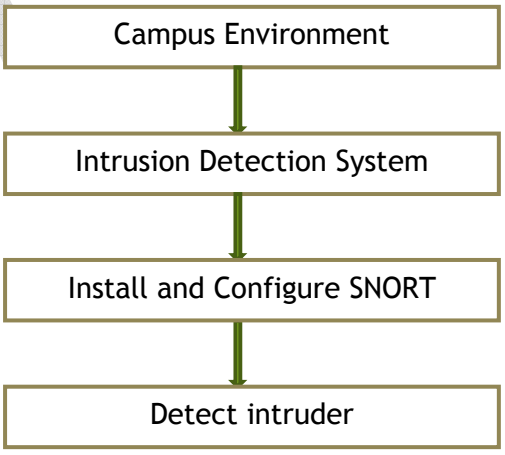
Mukta Garg

Assistant Professor, Advanced Educational Institutions, Palwal

Abstract

Today's society is totally dependent on network communications. Nobody wants to move a single step from his/her seat. Everyone does it's all over daily routine tasks via internet source only. So it is very important to maintain a security of high level over the network to ensure secure and trusted network communication because network data communication is always a matter of threat via attackers and intruders. During recent years, number of attacks on networks has increased so there is a need of reliable network and this is the current hot topic among researchers. My research proposal provides a review of various Intrusion Detection Systems and its tools by focusing on SNORT IDS-an open source tool. Also, I have presented an extension of SNORT IDS by adding a new pre-processor in snort detection engine to find the detection anomalies. This engine filters all the files and loads the attacked or infected files into its loader by .conf file command.

Keywords- IDS, SNORT, tools, detection engine, network security, attacks.



IJAETMAS

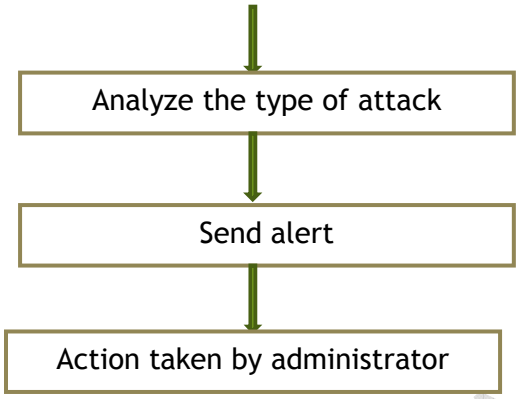


Figure 1: Flow of IDS in Campus Environment

1.0 Introduction

Intrusion detection System is an approach that discovers network errors or intrusions. Intrusion Detection is implemented by an Intrusion Detection System available today in the form of various tools. The attacks on network communication are increasing day-by-day and also becoming sophisticated. Due to huge and complex infrastructure of computer networks, it is very difficult to completely secure such networks. An intruder attacks on multiple nodes in LAN and may also move between nodes [16]. Intrusion detection is the act of detecting unwanted traffic on a network or on a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable used policies. Intruder may be a system, a person or a program that is illegally tries to break the Intrusion System. IDS have the task of monitoring the systems in a network and detect the insecure states or malware attacks.

Classification of Intrusion Detection System

Intrusion detection system is classified into two types:
1. Host based IDS
2. Network based IDS

1. Host based IDS (HIDS)

Host intrusion detection systems run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate [1].HIDS can use both anomaly and misuse detection system.

2. Network based IDS (NIDS)

NIDS are deployed on strategic point in network infrastructure. The NIDS can capture and analyze data to detect known attacks by comparing patterns or signatures of the database or detection of illegal activities by scanning traffic for anomalous activity. NIDS are also referred as "packet- sniffers", because it captures the packets passing through the communication mediums. Network intrusion detection systems are placed at the strategic points within the network to monitor traffic to and from all devices on the network. It performs an analysis for a passing traffic on the entire subnet, works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of known attacks. Once the attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator [1].

Comparison with firewalls

An intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm [1]. An IDS also watches for attacks that originate from within a system by matching signatures stored **as** patterns and generates an alert.

IDS use two main detection techniques:

Anomaly-based IDS

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline. The issue is that it may raise a False Positive alarm for a legitimate use of bandwidth if the baselines are not intelligently configured [16].

Signature-based IDS

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware [1].

Therefore, IDS have the task of monitoring the systems in a network and detect the insecure states or malware attacks. In this research, I am working with SNORT IDS. I proposed an architectural solution to implement the IDS via SNORT in a campus network environment. The objective of this implementation is to measure and detect then malware or SNORT application over LAN [2].

Brief Statement or Relevance of the Problem

In network communication, there are so many issues related with network security. Most threatened one is the security breach problems due to malware attacks and intruders. So many techniques were emerged like firewalls, cryptography, encoding, etc. but none of them is entirely successful for avoiding these malwares from attacks.
After then IDS came into picture. Though it became a successful tool for detecting and preventing intruders but some anomalies are still there like if we use any detection tool like SNORT, it works very well and is signature based but problem arises when there is a gap between a new threat coming instant having no detection signature stored previously in the database pattern. Therefore this type of new threat or attack will not be identified or detected by the tool. So my basic focus area will be to solve this issue if there is a lag. Secondly, IDS tool becomes weaker when there is high network traffic. Another main problem is related with SNORT architecture. We cannot understand the working of snort detection engine that where the defected files stored and how it filters the data. So, I have also presented an extension of SNORT IDS by adding a new pre-processor in snort detection engine to find the detection anomalies. This engine filters all the files and loads the attacked or infected files into its loader by .conf file command. Another two problems discussed above will be my future research work.

Objectives of the study

All the above papers discussed the way to use various IDS tools to detect intruders in the data network. My approach or proposed solution is to develop an improved algorithm by considering previously defined methodologies or to present an extension of SNORT IDS tool by adding a new pre-processor in snort detection engine to find the detection anomalies. This engine filters all the files and loads the attacked or infected files into its loader by .conf file command. With the help of this, an efficient detection can be done. However, security, accuracy and reliability will be the main concern during the detection process.

The main objective of the study is to analyze the Problems, Prospective and Opportunities of various aspects in IDSs. In this broader domain, the following will be specific objectives of the study:

1. To study the existing tools appropriately.
2. To find out the obstacles/problems faced by various IDSs.
3. To identify the capabilities of SNORT IDS.
4. To examine the results with the previous used approaches.
5. To find out the ways to improve the snort performance by increasing the power of network resources to stop packet dropping.
6. To survey the performance of snort as it becomes down during heavy network traffic.
7. To build a prototype model or a change in architectural design to filter and delete the intrusion attack automatically in real time network.

8. To raise an issue on the accuracy and reliability of the defects detected by IDSs. Sometimes missed attacks are there which are not detected by IDS and they entered in the network as IDS can't notice them.

Research Methodologies and Tools to be adopted

To carry out proposed research, a few techniques and tools shall be required for performing different tasks. A brief summary of these tools and techniques is given below. This is tentative not an exhaustive list. During research, if a new technique or tool is found, it may be integrated into the work. It is a planned list. Tools used are:

1. SNORT IDS.
2. SNORT Rules.
3. Windows or Linux OS.

SNORT IDS TOOL

It is a free and source network (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998.Martin Roesch released Snort. A Snort works as a packet sniffer. It means it captures and displays packets from the network with different levels of detail on the console.

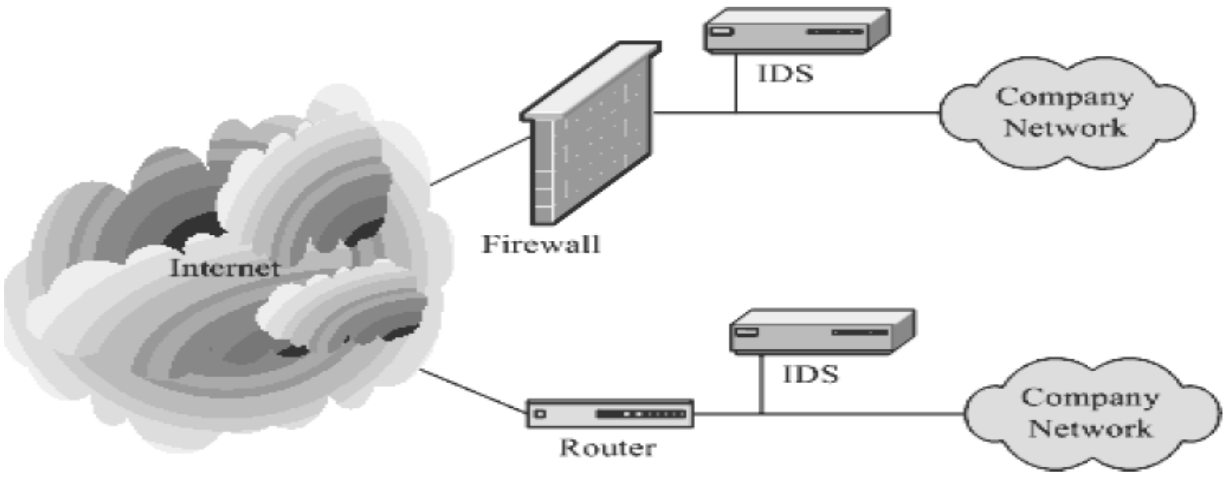


Figure 2: Typical locations for SNORT [9][15]

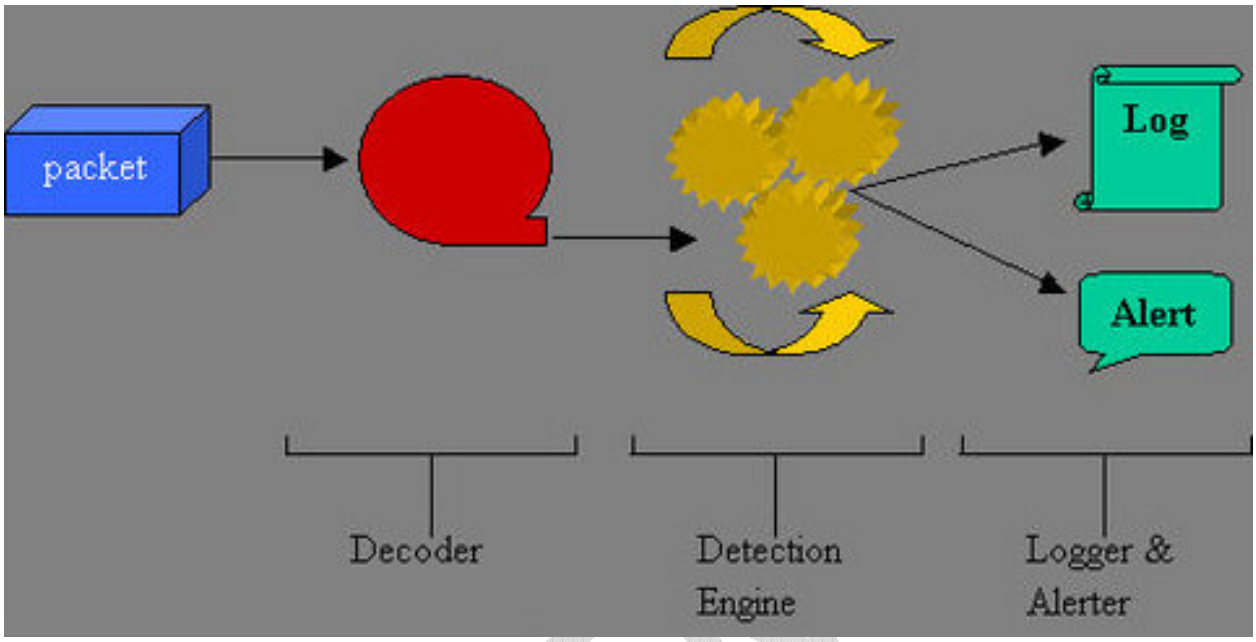


Figure 3: SNORT ARCHITECTURE [15][16]

SNORT COMPONENTS:

Working of Snort on Linux [6]

1. **Create the required files and directory**

You have to create the configuration file, rule file and the log directory [8].

Table: Rule structure and example	
Structure	Example
Rule Actions	Alert
Protocol	ICMP
Source IP Address	Any

International Journal of Advancement in Engineering Technology, Management & Applied Science
Volume 1, Issue 5 October 2014 ISSN No: 2349-3224

Source Port	Any
Direction Operator	->
Destination IP Address	Any
Destination Port	Any
(rule options)	(msg:"ICMP Packet"; sid: 477; rev: 3 ;)

Table 1

2**. Execute snort** [4]

snort -c /etc/snort/snort.conf -l /var/log/snort/

Execute snort as Daemon

Add -D option to run snort as a daemon.

snort -D -c /etc/snort/snort.conf -l /var/log/snort/

Additional Snort information [4][6]

Default config file will be available at snort-2.8.6.1/etc/snort.conf

From: http://www.snort.org/snort-rules

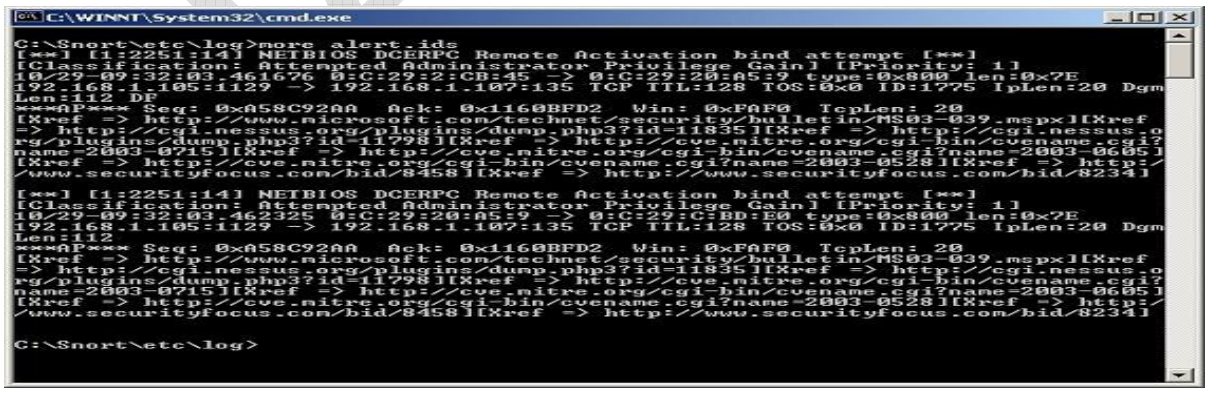

C:\WINNT\System32\cmd.exe
C:\Snort\etc\log>more alert.ids
[**] [1:2251:14] NETBIOS DCERPC Remote Activation bind attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
10/29-09:32:03.461676 0:C:29:2:CB:45 -> 0:C:29:20:A5:9 type:0x800 len:0x7E
192.168.1.105:1129 -> 192.168.1.107:135 TCP TTL:128 TOS:0x0 ID:1775 IpLen:20 Dgm
Len:112 DF
AP Seq: 0xA58C92AA Ack: 0x1160BFD2 Win: 0xFAF0 TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx][Xref
=> http://cgi.nessus.org/plugins/dump.php3?id=11835][Xref => http://cgi.nessus.o
rg/plugins/dump.php3?id=11798][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?
name=2003-0715][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0605]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0528][Xref => http:/
/www.securityfocus.com/bid/8458][Xref => http://www.securityfocus.com/bid/8234]
[**] [1:2251:14] NETBIOS DCERPC Remote Activation bind attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
10/29-09:32:03.462325 0:C:29:20:A5:9 -> 0:C:29:C:BD:E0 type:0x800 len:0x7E
192.168.1.105:1129 -> 192.168.1.107:135 TCP TTL:128 TOS:0x0 ID:1775 IpLen:20 Dgm
Len:112
AP Seq: 0xA58C92AA Ack: 0x1160BFD2 Win: 0xFAF0 TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx][Xref
=> http://cgi.nessus.org/plugins/dump.php3?id=11835][Xref => http://cgi.nessus.o
rg/plugins/dump.php3?id=11798][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?
name=2003-0715][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0605]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0528][Xref => http:/
/www.securityfocus.com/bid/8458][Xref => http://www.securityfocus.com/bid/8234]
C:\Snort\etc\log>

Figure 4: Working of Snort [4]

Why we would choose Snort over other ID systems [1][9]:-

1) Snort is passive, which leads it to monitor any system on your network with no configuration to the target computer.
2) Portable and Fast.
3) Snort is able to log to numerous databases include Oracle, Microsoft SQL Server, MySQL, and Postgre SQL.
4) Flexible and simple, Snort uses plugins for all of its functions so you could drop plugins and remove them as you wish.
5) Snort rule file (signatures) are easy to write and are effective.
6) Snort is ported to every major operating system.

Problem with snort

Some problems are raised when we tried to start the snort service on Linux. This issue started to happen when we updated rules .So, when we try to start snort manually we get the following error [18]:

ERROR: Warning: /etc/snort/rules/netbios.rules (24) => Unknown keyword' dce_iface' in rule!

ERROR: Unable to open rules file "/etc/snort//etc/snort/rules/local.rules": No such file or directory.

However, it can be removed by using:

First of all create your /etc/snort/rules/icmp.rules
then modify /etc/snort/snort.conf in the following way:

cat /etc/snort/snort.conf
include rules/icmp.rules

Other Problem with snort architecture

In last years, some projects have been proposed to extend the capabilities of Snort. For instance, models only the http traffic, models the network traffic as a set of events and look for abnormalities in these events, enhance the functionalities of Snort to automatically generate patterns of misuse from attack data, and the ability of detecting sequential intrusion behaviors, that is a pre-processor based on studying the defragmentation of package in the network to avoid evasive attacks in the IDS. However, it is advisable to design a hybrid system to model the network traffic in a high level.

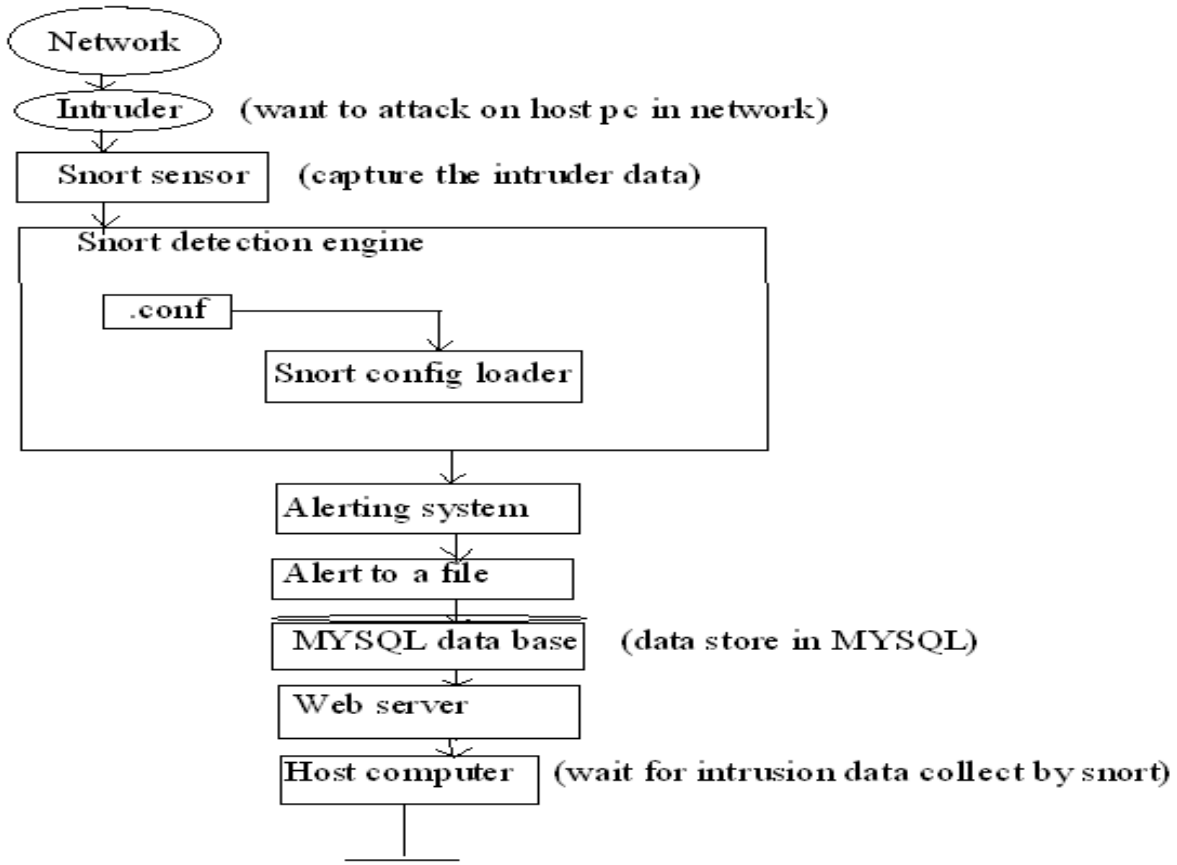


Figure 5: Working of SNORT after pre-processor extension

Proposed solution of problem - a New Hybrid IDS: H-Snort

As indicated above, my research has designed a pre-processor to allow detection of anomalies that converted Snort into a hybrid system. This system, named H-Snort meets the various requirements easily [5].

Snort has been extended by adding an anomaly detection pre-processor which access to a database MySQL where it is centralized the system configuration, statistical data and anomalies detected by the system. The system is complemented by a website that displays the system status (network traffic, detected anomalies, etc.) and that also allows to configure the system easily.

References, Bibliography, Webliography and list of works cited

[1] http://books.google.co.in

[2] Ismail, M. N. and Ismail, M. T.; "Framework of Intrusion Detection System via SNORT application on Campus Network Environment", proceedings of IEEE International Conference on "Future Computer and Communication", pp: 455-459, 2009.

[3] Salah, K. and Kahtani, A.; "Improving SNORT performance under LINUX", Proceedings of Communications, IET, vol 3, Issue: 12, pp: 1883-1895, 2009.

[4] Suman Rani and Vikram Singh; "SNORT: An Open Source Network Security Tool for Intrusion Detection in Campus Network Environment", proceedings of IJCTEE, Volume 2, Issue 1(ISSN 2249-6345)

[5] Prathibha. P. G. and Dileesh. E. D.; "Design of a Hybrid Intrusion Detection System using SNORT and HADOOP", proceedings of International Journal of Computer Applications (0975-8887) Volume 73-No. 10, July 2013, pp: 5-10, 2013.

[6] Vinod Kumar and Dr. Om Prakash Sangwan "Signature Based Intrusion Detection System Using SNORT", proceedings of International Journal of Computer Applications and Information Technology, Vol. I, Issue III, November 2012(ISSN: 2278-7720), pp: 35-41, 2012.

[7] R. Henders and B. Opdyke. "Detecting Intruders on a Campus Network: Might the Threat Be Coming From Within?", User Services Conference, Monterey, Proceedings of the 33rd annual ACM SIGUCCS Conference on User Service, CA, USA, 2005, pp: 113-117.

[8] M. Roesh."SNORT-Lightweight Intrusion Detection for Networks", Proceedings of LISA99, the 13th System Administration Conference. 1999.

[9] SNORT IDS. Available at http://www.snort.org/-August 2006.

[10] Mukherjee, B., Heberlein, L. T. and Levitt, K. N.; "Network Intrusion Detection", Proceedings of IEEE International Conference on "Network" vol. 8, Issue: 3, pp: 26-41, 1994.

[11] Brian Caswell and Jeremy Hewlett. Snort User's Manual (http://www.snort.org/docs/)

[12] Beale, J. and Foster, J. C. SNORT 2.0 Intrusion Detection. Syngress Publishing, 2003.

[13] Peyman Kabiri and Ali. A. Ghorbani, "Research on Intrusion detection and Response: A Survey", Proceedings of International Journal of Network Security, vol. 1, No. 2, pp: 84-102, Sep. 2005(http://isrc.nchu.edu.tw/ijnsl).

[14] Webliographyhttp://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview.

[15] Yue Jiang "Snort - a network intrusion prevention and detection system".www.csee.wvu.edu/~cukic/CS665/**Snort**.ppt.

[16] Trushna T. Khose Patil and C. O. Banchhor, "Distributed Intrusion Detection System using m6bile agent in LAN environment", Proceedings of International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2013, pp:1901-1903.

[17] Intrusion detection system - Wikipedia, the free encyclopedia.html.

[18] http://www.thegeekstuff.com/2010/08/snort-tutorial/

IJAETMAS